Superhighway robbery Internet-based scam artists can turn your company's PCs against you. BY KEVIN SAVETZ

If you learned that an employee was leaking company secrets or stealing your customers' credit card numbers, you would certainly fire the worker on the spot. Your computers may be doing just that – with the unwitting help of your employees.

Programs hidden in your company's personal computers could be sharing documents, customer data, or even everything that is typed on a keyboard with the outside world. It's possible that someone outside the company can take control of the computer, using it to send spam, spy on your employees, or erase your data on a whim.

These invasions probably aren't coming from your competition in an espionage scheme. They most often come from complete strangers and start when an employee installs a useful-sounding application or is tricked by a scam aimed at thousands of potential victims.

"The average employee is very naive about information security," says Mike Tansey, president of Vision Computer Services and a member of the Rotary Club of Sylvania, Ohio, USA. Tansey's company offers network and communications consulting to small businesses. "Employees are not aware of the wide variety of attack methods used to compromise their security. Unfortunately, most business owners are just as uninformed about risks."

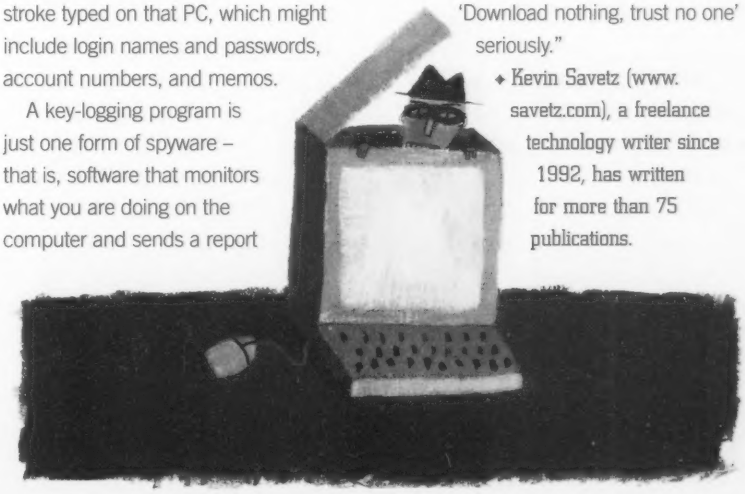
Devious folks can find many ways to squeeze information from your company. Some prey on technical deficiencies. Others aim for people, who are often an easier target. Tansey says most employees have never heard of the security threats they face, like social engineering, phishing, key loggers, and spyware.

Social engineering is a fancy name for basic trickery. A cracker who wants a password might call an office manager pretending to be a technician needing the password to fix a problem.

Phishing is the use of misleading e-mails and fraudulent Web sites to collect private information. If you receive an e-mail message from a bank asking you to log in to verify your account information, it's likely a phishing attempt.

A key logger is hidden software or hardware that keeps track of every keystroke typed on that PC, which might include login names and passwords, account numbers, and memos.

A key-logging program is just one form of spyware – that is, software that monitors what you are doing on the computer and sends a report to its maker. A survey of computer users by the National Cyber Security Alliance and America Online found that 80 percent of home computers were infected with spyware. Anti-spyware software like Spybot Search & Destroy (free, www.safer-networking.org/en/) can get rid of common spyware infections, but can't undo their damage. Teach employees not to install unapproved software so spyware doesn't get a foothold.

"Changing your password daily will not help you if you have spyware installed on your PC sending out that password to a thief," Tansey says.The answer to all of these problems is professional education and companywide security policies. "A comprehensive, written security policy is crucial for businesses today," he says. "Employees need to be educated about the risks that the business faces," Tansey says, adding that proper education will "show all staff what can happen if they don't take the new policy of 'Download nothing, trust no one' seriously."

◆ Kevin Savetz (www.savetz.com), a freelance technology writer since 1992, has written for more than 75 publications.